REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is directed to non-statutory subject matter under 35 U.S.C. §101, fails to comply with the written description requirement under the provisions of 35 U.S.C. §112, or is obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

In addition, the Applicants' representative would like to thank Examiner Moorthy for kindly taking a substantial amount of time on May 14, 2009 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. REJECTION OF CLAIMS 10-12 UNDER 35 U.S.C. §101

Claims 10-12 stand rejected as being allegedly directed to non-statutory subject matter. In response, the Applicants have amended independent claims 10-12 in order to more clearly recite aspects of the present invention.

Specifically, the Applicants have amended independent claims 10-12 to recite a "sensor device containing an executable program," replacing "a computer readable storage medium containing an executable program." The Applicants respectfully submit that a sensor device is clearly an apparatus, and, therefore, constitutes statutory subject matter within the meaning of 35 U.S.C. §101.

Therefore, the Applicants respectfully submit that claims 10-12 fully satisfy the requirements of 35 U.S.C. §101. Accordingly, the Applicants respectfully request that the rejection under 35 U.S.C. §101 be withdrawn.

II. REJECTION OF CLAIMS 10-12 UNDER 35 U.S.C. §112

Claims 10-12 stand rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. In response, the Applicants have amended independent claims 10-12 in order to more clearly recite aspects of the present invention.

Specifically, as discussed above, the Applicants have amended independent claims 10-12 to recite a "sensor device containing an executable program," replacing "a

computer readable storage medium containing an executable program." The Applicants respectfully submit that the use of such sensors is described throughout the Specification, for example at least in Sections I and II ("Introduction" and "Intrusion Detection With Correlated Sensors"), and is illustrated in the Drawings at least in Figures 1 and 3.

Therefore, the Applicants respectfully submit that claims 10-12 fully comply with the written description requirement of 35 U.S.C. §112, first paragraph. Accordingly, the Applicants respectfully request that the rejection under 35 U.S.C. §112 be withdrawn.

III. REJECTION OF CLAIMS 1-5, AND 10-12 UNDER 35 U.S.C. § 103

Claims 1-5 and 10-12 stand rejected as being unpatentable over the Baba patent (U.S. 7,051,369, hereinafter "Baba") in view of the Fox et al. patent (U.S. 7,096,502, hereinafter "Fox"). In response, the Applicants have amended independent claims 1, 4, 5, and 10 – 12 in order to more clearly recite aspects of the present invention.

Particularly, the Examiner's attention is directed to the fact that Baba and Fox, singly or in any permissible combination, fail to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding current states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12.

The Examiner acknowledges that "Baba does not teach the firewall and sensor [disclosed by Baba] are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall." (Office Action, Page 6) However, the Examiner submits that Fox bridges this gap in the teachings of Baba. The Applicants respectfully disagree.

By contrast, Fox discloses a system for assessing the security of a network that determines a probability that an event (*e.g.*, an attack) will occur in the network in the future. For instance, column 12, lines 32-35 of Fox state that the system projects the state of the computer system network "into the future and draws inferences about threats, vulnerabilities, and opportunities for operation" (emphasis added). In other words, the "probability" referred to by Fox is the likelihood that an attack on the network will occur. Thus, the "probabilistic belief" disclosed by Fox relates neither to a state of a

system resource of service (by contrast, it relates to a network event) nor to a current observation (by contrast, it relates to a predicted future occurrence), as clearly claimed by the Applicants.

Specifically, Applicants' claims 1, 4, 5, and 10 - 12 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to a suspicious activity in the intrusion detection system is improved. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

5. A method for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of

services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

10. A sensor device containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to a suspicious activity in the intrusion detection system is improved. (Emphasis added)

11. A sensor device containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

12. A sensor device containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the first sensor

so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

As discussed above, Baba in view of Fox fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding current states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Therefore, the Applicants submit that independent claims 1, 4, 5, and 10 - 12 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-3 depend from claim 1 and recite at least the same patentable features recited in claim 1. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2-3 are also not obvious over the teachings of Baba in view of Fox. Therefore, the Applicants submit that dependent claims 2-3 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

IV. STATEMENT OF SUBSTANCE OF INTERVIEW OF MAY 14, 2009

In response to the Interview Summary dated May 15, 2009, the Applicants submit the following statement regarding the substance of the interview of May 14, 2009:

A) No exhibits or demonstrations were conducted.

B) Claims 1 and 10-12 were discussed.

C) The Fox reference (U.S. 7,096,502) was discussed.

D) The Applicants' representative agreed to amend the independent claims in order to clarify that the claimed "belief states" of the sensors pertain to the current states of the monitored resources or services, as opposed to predictions of the likelihoods of future events. In addition, the Applicants' representative agreed to amend claims 10-12 to refer to "sensor devices" in order to overcome the rejections under 35 U.S.C. §101 and 35 U.S.C. §112.

E) The Examiner's Interview Summary correctly describes the substance of

the interview.

F) No other pertinent matters were discussed.

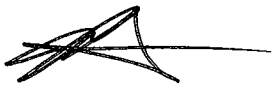
G) The Examiner and the Applicants agreed that the proposed amendment would be implemented in the Applicants' response to the present Office Action.

V. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §101, 35 U.S.C. §112, and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 842-8110 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,



May 26, 2009
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 842-8110

Wall & Tong, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702